AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A Dell XPS D14M tower computer, Service Tag: 3FPBJB2, Express Code: 7479868286 located in the USSS, Cincinnati Field Office's Evidence Vault, 550 Main St., #10-503, Cincinnati, OH 45202

Case No. 3:17mj370

MICHAEL J. NEWMAN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1343	Wire Fraud
18 U.S.C. 1029 and 1029A	Identity Fraud and Access Device Fraud
18 U.S.C. 371 and 1349	Conspiracy

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

J Teuschl
Applicant's signature

SA James Teuschl
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/14/17

Judge's signature

City and state: DAYTON, OHIO

MICHAEL J. NEWMAN, U.S.MAGISTRATE JUDGE
Printed name and title

AFFIDAVIT

1) I, James Teuschl, being duly sworn, depose and state that I have been a Special Agent with the United States Secret Service (USSS) since September 2000. I have previously received training in the investigation of violations of various white-collar federal crimes to include: counterfeiting, wire fraud, identity fraud, access device fraud and conspiracy. I am currently assigned to the USSS Cincinnati, Ohio Field Office. Prior to my current employment with the USSS, I was employed by the State of Ohio as a Parole Officer.

2) This affidavit is submitted in support of applications for search warrants authorizing the forensic examination of four (4) cellular phones/iPod and one (1) computer tower. Each of these items were seized by law enforcement officials on August 8, 2017 in conjunction with the execution of a federal search warrant issued on August 3, 2017 by U.S. Magistrate Judge Michael Newman in Case No. 3:17-mj-355. Each of the four items were seized at or near a residence located at 3122 Benninghofen Ave, Hamilton, OH 45015.

3) Because this affidavit is provided for the limited purpose of establishing probable cause for the requested search warrant, I have not included all factual details known to this investigation. I have opted to only include those facts deemed sufficient to establish probable cause for the sought after search warrant. The following information is either personally known to me, or was reported to me by other law enforcement officers familiar, and/or involved with this investigation.

4) It is suspected that individuals identified as Joshua Leavell and Cabel Leavell III have been engaged in a scheme and artifice to defraud various Sam's Clubs located throughout the Southern District of Ohio ("SDOH") by committing acts of wire fraud (18 U.S.C. 1343); identity fraud (18 U.S.C. 1029); access device fraud (18 U.S.C. 1029A) and conspiracy (18 U.S.C. 371 and 1349). I believe that that certain evidence, fruits, and instrumentalities of such violations may be currently located at the above-described residence, in surrounding curtilage and in adjoining parked vehicle(s).

5) It is further suspected that Joshua Leavell, Cabel Leavell III and other unknown individuals have engaged in this fraudulent scheme beginning in early 2017 and continuing up to and including April 3, 2017. Sam's Clubs are owned and operated by the Walmart Corporation of Bentonville, AR.

Summary of the Fraud Scheme

1) The Walmart Corporation (DBA Sam's Club) operates a chain of member's only shopping clubs located throughout the United States. Patron members pay a yearly fee for the privilege of shopping at Sam's Clubs. Patron members have the ability to join the Sam's Club Plus Members Program, which allow participant members to accrue "cash rewards" from qualifying retail purchases. Earned "cash rewards" are thereafter electronically loaded onto the individual's member's account. At the end of each year (12 month period) accumulated "cash rewards" are tallied up and then made available for redemption by the participant member for cash or credit.

2) According to Walmart Global Investigations ("WGI") representatives Trent Peebles, Michael Warren, Leslie Self and Emily Young; (all of whom are based out of Bentonville, AR), on or about April 2017, Walmart Corporate officials learned that various Sam's Club members had their accumulated "cash rewards" accounts illicitly accessed and drained. The victim participant Sam's Club members reside in various locations throughout the United States.

3) WGI was able to identify certain individuals who had used internet websites and social media web pages to improperly purchase and sell Sam's Club "cash rewards" accounts. Sam's Clubs member account numbers and corresponding account password(s) were being offered for sale on said websites at 20-25% of the face value of the "cash rewards."

4) When Sam's Club Plus Members reported losses to their "cash rewards accounts," Walmart Corporation (DBA Sam's Club) issued 100% refunds for the claimed stolen "cash rewards" amount(s).

5) According to WGI representatives, the Walmart Corporation (DBA Sam's Club) specifically identified two male individuals at Sam's Clubs in the SDOH who were improperly utilizing "cash rewards" Plus Member's points to purchase large amounts of ITunes Gift Cards. WGI investigators determined that the two said male suspects utilized cellular smartphones to log onto "cash rewards" Plus Member accounts via internet. The observed illicit purchase transactions primarily took place at self-checkout kiosks located in the various Sam's Clubs. These transactions were paid for with multiple members' stolen "cash rewards" accounts, none of which the two suspects were authorized to access or use.

6) In February 2017, an employee at Sam's Club #6528, located at 815 Clepper Lane, Cincinnati, OH 45245, observed the two male suspects depart the store in a blue 1999 GMC Suburban, VIN 3GKEC16RXXG511217, which had been parked outside the store. Said vehicle displayed OH license plate

EVV4560. WGI investigators subsequently conducted a TransUnion Credit database search of said vehicle and license plate. This search revealed the subject vehicle was registered to Cabel Leavell III, of 3122 Benninghofen Ave, Hamilton, OH 45015. An additional database search by WGI officials yielded photos of Joshua Leavell and Cabel Leavell III, both of which matched the subject individuals previously observed appearing in Sam's Club video surveillance engaging in suspected fraudulent "cash rewards" transactions.

7) WGI representatives thereafter began reviewing and compiling video surveillance from various Sam's Clubs located in the SDOH involving suspected fraudulent "cash rewards" transactions. As a result, WGI officials were able to link Joshua Leavell and Cabell Leavell III to numerous other fraudulent transactions occurring at various SDOH Sam's Club locations during the January-April 2017 time frame. Joshua Leavell was repeatedly observed appearing in video surveillance footage utilizing a cellular smartphone to log onto "cash rewards" accounts at checkout registers. Cabel Leavell III was also observed concealing items on his person after the transactions were completed.

8) WGI representatives have identified Joshua Leavell and Cabel Leavell III as being responsible for approximately $14,544.49 in fraudulent "cash rewards" transactions committed at Sam's Club #6528, located at 815 Clepper Lane, Cincinnati, OH 45245, from January 19, 2017 through February 4, 2017.

9) WGI representatives have identified Joshua Leavell and Cabel Leavell III as being responsible for approximately $2,991.35 in fraudulent "cash rewards" transactions committed at Sam's Club #6544, located at 9570 Fields Ertel Road, Loveland, OH 45140, from February 4, 2017 through February 5, 2017. During said time frame, Joshua Leavell and Cabel Leavell III notably purchased home fitness equipment using "cash rewards" and thereafter had said fitness equipment delivered to their confirmed address of 3122 Benninghofen Ave, Hamilton, OH 45015, with their name on receipt.

10) WGI representatives have identified Joshua Leavell and Cabel Leavell III as being responsible for approximately $6,680.33 in fraudulent "cash rewards" transactions committed at Sam's Club #8136, located at 1111 Miamisburg Centerville Road, Washington Township, OH 45459, from March 3, 2017 through April 3, 2017.

11) WGI representatives have identified Joshua Leavell and Cabel Leavell III as being responsible for approximately $14,107.36 in fraudulent "cash rewards" transactions committed at Sam's Club #6517, located at 3446 Pentagon Blvd, Beavercreek, OH 45431, from March 4, 2017 through March 25, 2017.

12) WGI representatives have identified Joshua Leavell and Cabel Leavell III as being responsible for approximately $13,908.58 in fraudulent "cash rewards" transactions committed at Sam's Club #6380, located at 6955 Miller Lane, Dayton, OH 45414, from March 8, 2017 through April 2, 2017.

13) The Walmart Corporation (DBA Sam's Club) reports an estimated loss to date of at least $104,464.11, directly attributed to suspected fraudulent "cash rewards" transactions committed by Joshua Leavell and Cabell Leavell III.

14) On March 28, 2017, the Montgomery County Sheriff's Office received a report from a Sam's Club members complaining of fraudulent "cash rewards" transactions. As a result, Sheriff's Detective Linda Shutts began tracking losses and gathered video surveillance from various Sam's Club store locations. Two male suspects were later identified as Joshua Leavell and Cabel Leavell III.

15) On April 3, 2017, a Sam's Club manager observed both said suspects at the Sam's Club, located at 1111 Miamisburg Centerville Road, Washington Township, OH 45459. Law enforcement officials were notified and Montgomery County Sheriff Deputies thereafter arrested Joshua and Cabel Leavell III without incident. State identity fraud charges were thereafter filed.

16) On April 5, 2017, Montgomery County Sheriff's Detective Shutts executed a state search warrant on Joshua Leavell's white 2017 Toyota *Sienna* minivan, VIN 5TDDZ3DC3HS151260. Said vehicle displayed OH license plate # GOH 1585. This search yielded additional receipts/merchandise from Dayton area Sam's Clubs "cash rewards" purchases and Kohl's stores "cash rewards" purchases.

17) On July 7, 2017, USSS Special Agents Jeffrey Schmitz and James Harris conducted a surveillance of 3122 Benninghofen Ave, Hamilton, OH 45015. Agents Schmitz and Harris observed both said parked at subject residence.

18) On July 24, 2017, your Affiant conducted a search of the Law Enforcement Vehicle Sighting database concerning Joshua Leavell's Toyota *Sienna* van, Ohio license plate # GOH 1585. Between October 20, 2015 through July 24, 2017 there were 13 separate sightings of this vehicle parked outside of 3122 Benninghofen Ave, Hamilton, OH 45015 residence.

19) On July 24, 2017, your Affiant conducted a records search of the Butler County Auditor's database concerning 3122 Benninghofen Ave, Hamilton, OH 45015. This search revealed that the listed owners of this residence are Cabel D Leavell III and Cindy Lynn Leavell.

20) Based on your Affiant's prior training and experience investigating similar wire fraud, identity fraud, access device fraud, and conspiracy cases, your Affiant believes:

a. That individuals involved in identity fraud, access device fraud and conspiracy cases such as subject case, typically convert fraudulently acquired goods into cash or similar formats. To accomplish this goal, the fraudulently acquired goods are often resold to third parties; individually or in bulk. Payment for said items are commonly made in the form of cash, wire transfer or bitcoins.

b. That it is common for individuals involved in identity fraud, access device fraud and conspiracy cases such as subject case typically maintain lists and records of victim stores, purchases, names, addresses, account numbers, and/or telephone numbers of their customers, victims and associates, in books, paper notes, notebooks, computer files, telephone texts, digital address books and/or papers.

c. That it is common for individuals involved in identity fraud, access device fraud and conspiracy cases such as subject case to maintain, hide and leave said items in their residences and motor vehicles in order to prevent their discovery by law enforcement officials. These locations are additionally used because such individuals engaged in such illicit behavior feel these locations are secure and generally protected from third party access and scrutiny. These locations are easily maintained by criminals for ready and easy access.

21) On August 8, 2017, Special Agents of the USSS, U. S. Department of Agriculture-OIG, Ohio Investigative Unit and officers from the Hamilton Police Department participated in the execution of said federal search warrant on the residence located at 3122 Benninghofen Ave, Hamilton, Oh 45015. During the course of executing said search warrant, Joshua Leavell specifically consented to a search of his blue 2017 Toyota *Prius* and white 2017 Toyota *Sienna* van, both of which were then parked at a curbside located adjacent to said residence.

22) During the course of said searches, a Dell XPS D14M tower computer, Service Tag: 3FPBJB2, Express Code: 7479868286 was seized from said residence; an Apple iPhone Model A1661, FCC ID BCG-E3087a, IC: 579C-E3087A was seized from the person of Joshua Leavell; a ZTE cellular phone Model Z233VL; serial # 329F74827279 was seized from said *Prius* automobile; a Motorola cellular smartphone Model Moto G, serial # SJUG7178AA, Track ID ZY22WZRNP was seized from said *Prius* automobile; and an Apple iPod Model A1574, serial # CCQT31N3GGK4 was seized from said *Sienna* van.

23) As part of this search, law enforcement officials seized large quantities of prepaid gift cards and cashier checks bearing large dollar amounts from the said blue 2017 Toyota *Prius*.

TECHNICAL TERMS

24) Based on my training and experience, I use the following technical terms to convey the following meanings:

A. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

B. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

C. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as

personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

D. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

E. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

F. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

G. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

25) Based on my training, experience, and research, I know that the four previously described and seized Devices have respective capabilities that allow it to access the internet to the extent that they support probable cause. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26) Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that

have been viewed via the Internet are typically stored for some period of time on various electronic devices such as the four seized devices. This information can sometimes be recovered with forensics tools.

27) There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

A. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

C. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

D. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28) *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

B. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

C. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

F. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime

of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

29) *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30) *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

31) Each of the said three (4) cell phones/iPod and one (1) tower computer are presently stored and secured at the USSS, Cincinnati, OH Field Office evidence vault which is located at 550 Main Street, Room #10-503, Cincinnati, Ohio 45202.

32) Based on your Affiant's prior training and experience investigating similar wire fraud, identity fraud, access device fraud and conspiracy cases, your Affiant has concluded that there is probable cause to believe that these three said cell phones and tower computer in all likelihood contain data and information that amounts to evidence, fruits, and instrumentalities of aforesaid criminal violations.

33) Wherefore, your Affiant respectfully requests that search warrants be issued authorizing the USSS, to forensically examine any and all stored data contained in and on the aforesaid five electronic components set forth and more fully described in Attachment B.

Further your Affiant sayeth naught.

James Teuschl,
Special Agent, United States Secret Service

Subscribed and sworn to before me on this 14th day of August, 2017.

MICHAEL NEWMAN
United States Magistrate Judge

ATTACHMENT "A"

Property/Location to be Searched

Relevant items of previously seized evidence listed in Attachment "B" which are presently stored and secured in the USSS, Cincinnati Field Office's Evidence Vault, maintained and located at 550 Main St., #10-503, Cincinnati, OH 45202.

ATTACHMENT "B"

Items to be Searched

a. A Dell XPS D14M tower computer, Service Tag: 3FPBJB2, Express Code: 7479868286.
b. An Apple iPhone Model A1661, FCC ID BCG-E3087a, IC: 579C-E3087A.
c. A ZTE cellular phone Model Z233VL, serial # 329F74827279.
d. A Motorola cellular smartphone Model Moto G, serial # SJUG7178AA, Track ID ZY22WZRNP.
e. An Apple iPod Model A1574, serial # CCQT31N3GGK4.